TITLE

A method and device relating to security in a radio communications network.

TECHNICAL FIELD

Embodiments of the invention relate to a method and device relating to security in a radio communications network, particularly a low power radio communications network.

BACKGROUND OF THE INVENTION

Security keys are generally used in a radio communications network to authenticate users or devices and to encrypt data communicated in the network. This prevents one user or device masquerading as another user or device. It also prevents eavesdropping on communications in the network. A security key is a data string that is secret i.e., not generally known to users of the network.

Typically a control device manages the security keys of a network. When a new device attempts to join the network, the user of the control device tells the user of the new device a secret. e.g. a PIN. The user of the control device manually inputs the secret PIN to the control device and the user of the new device manually inputs the same secret PIN to the new device. The control device and the new device separately and symmetrically create a secret security key. This security key is necessary for authentication of the new device and/or encryption of communications between the devices.

When another new device attempts to join the network, the same process occurs except a different PIN is generally used.

Such security measures are, for example, used in a Bluetooth® piconet. The control device is a low power radio frequency transceiver device operating as a Master. The new device is a low power radio frequency transceiver device attempting to join the piconet as a Slave. The security key is an initialization key Kinit created during the Link Manager Protocol (LMP) pairing process. In Bluetooth, encryption and authentication use different keys and the

initialisation key Kinit is used to ensure that a common link key, used in the authentication process, is shared by the Master device and the new Slave device.

It will therefore be appreciated to be disadvantageous that a user of the control device must enter data every time a new device attempts to join the network.

The inventors have realised that the user of the control device, if occupied in some other activity, must interrupt that activity to inform the new user of a new secret and enter the new secret to the device. This is particularly disadvantageous if the activity requires real time input such as a game.

BRIEF SUMMARY OF THE INVENTION

According to one aspect of the present invention there is provided a method of joining a first device to a radio communications network controlled by a second device without contemporaneous user input of a secret at the second device, comprising: storing in the second device a secret generated at the second device; making the stored secret available at the first device; and creating in the first device and in the second device, using the secret, a secret key for use in securing communication between the first and second devices.

According to another aspect of the present invention there is provided a method of joining a plurality of first devices to a radio communications network controlled by a second device, comprising: storing in the second device a generated secret at the second device; making the stored secret available to each of the first devices; and creating in the first devices and in the second device, using the secret, at least one secret key for use in securing communication between the first devices and the second device.

According to another aspect of the present invention there is provided a device for controlling a radio communications network comprising the device and one or more additional devices, the device comprising: a user interface

for generating a secret by user input; a memory for storing a generated secret for use in securing communications in the network; a radio transceiver for communicating in the network; and a processor for accessing the secret stored in the memory and for creating, using the accessed secret, a secret key for securing communication.

According to another aspect of the present invention there is provided 31. A radio communications network having a common secret for re-use in securing communications in the network, the network comprising : a controlling device, for creating the network, comprising: a user interface for user input of a common secret; a memory for storing a common secret; a first radio transceiver for communicating in the network; and a first processor for accessing the common secret stored in the memory and for creating, using the accessed common secret, a secret key for securing communication, and a participating device, for participating in the network, comprising: input means for inputting the stored common secret to the participating device; a second radio transceiver for communicating in the network; and a second processor for creating, using the input common secret, the secret key for securing communication.

According to another aspect of the present invention there is provided a radio communications network having a common secret for re-use in securing communications in the network, the network comprising a controlling device, for creating the network, comprising: a user interface for user input of a common secret; a memory for storing a common secret; a first radio transceiver for communicating in the network; and a first processor for accessing the stored common secret in the memory and for creating, using the stored common secret, secret keys for securing communication between the controlling device and each of a plurality of participating devices, and a plurality of participating devices, for participating in the network, each comprising: input means for inputting a common secret to the participating device; a second radio transceiver for communicating in the network; and a second processor for creating, using the input common secret, a secret key

for securing communication dependent upon the participating device and identical to one of the secret keys created in the controlling device.

It should be appreciated that although in embodiments of the invention, a first device is capable of being joined to a radio communications network controlled by a second device without contemporaneous user input of a secret at the second device, such embodiments do not exclude the possibility that it is also possible for a third device to be joined to the radio communications network controlled by the second device with contemporaneous user input of the same or a different secret at the second device. For example, while the third device is being joined to the network the user may contemporaneously input a secret, which is stored and re-used when the first device is subsequently joined to the network. The storage and re-use of the secret obviates the need for contemporaneous input of the secret when the first device is subsequently joined to the network.

BRIEF DESCRIPTION OF DRAWINGS

For a better understanding of the present invention reference will now be made by way of example only to the accompanying drawings in which:

Fig. 1A illustrates a Bluetooth piconet;

Fig. 1B illustrates a Bluetooth scatternet;

Fig. 2 illustrates a radio transceiver device in detail;

Fig. 3A illustrates a decision process according to one implementation of the present invention; and

Fig. 3B illustrates a decision process according to another implementation of the present invention; and

Fig. 4 illustrates the pairing process according to one aspect of the present invention.

DETAILED DESCRIPTION OF EMBODIMENT(S) OF THE INVENTION

Fig 1A illustrates a low power radio communications network 10 (a piconet) comprising a plurality of low power radio transceiver devices 2A, 2B, 2C and 2D. The network is a 'star' network topology. The radio transceiver device 2A operates as a Master and the radio transceiver devices 2B, 2C and 2D operate as Slaves. The Master M establishes and controls the network 10 and the plurality of Slaves S participate in the network 10. The Slaves S do not communicate directly with each other. Each Slave S can only communicate with the Master M.

Fig. 1B illustrates a low power radio communications network 10 (a scatternet) comprising a plurality of low power radio transceiver devices 2A, 2B, 2C and 2D in a first piconet 6 and a plurality of low power radio frequency transceiver devices 2D, 2E and 2F in a second piconet 8. The first piconet 6 is a "star" network topology. The radio transceiver device 2A operates as a master and the radio transceiver devices 2B, 2C and 2D operate as slaves. The second piconet 8 is also a "star" network topology. The radio transceiver device 2D operates as a master and the radio transceiver devices 2E and 2F operate as slaves. In this scatternet topology, the low power radio transceiver device 2D operates as a slave in the first piconet 6 and operates as a master in the second piconet 8. It joins the first and second piconets to form the scatternet. The master M establishes and controls its piconet and the plurality of slaves S in the piconet do not communicate directly with each other. Each slave S can only communicate with the master M of the piconet.

The above described networks 10 are Bluetooth networks (a piconet in Fig. 1A and a scatternet in Fig. 1B) and each radio transceiver device operates in accordance with the Bluetooth Standard. A Bluetooth radio transceiver device must be 'paired' with a Master M before it can join the network. The pairing process includes the creation of a common link key, using a shared PIN, that

is then used for authentication. In a piconet the same shared PIN is used for all the devices of the piconet. In a scatternet the same PIN is used for all the piconets of the scatternet.

Fig. 2 illustrates the radio transceiver device 2A in more detail. The device 2A comprises a processor 10, a low power radio frequency transceiver 12, a memory 14 and a user interface 16. The user interface 16 comprises a display 17 that receives control signals from the processor 10 and an input device 18, such as a keypad, that provides control signals to the processor 10. The processor 10 is operable to write to and read from the memory 14. The processor 10 is also connected to the low power radio transceiver 12 to which it provides data for transmission in the network 10 and from which it is provided with data received from the network 10.

The memory 14 stores a shared secret PIN 15. The PIN is 'shared' because it is known to the users or devices that should be able to join the network. It is re-used in the pairing process when such a device joins the network. The PIN is 'secret' because it is not otherwise known. To prevent it becoming known it is generally distributed without communication within the network 10. This means, for example, that the PIN is communicated orally between the users.

The shared secret PIN, which is typically a string of alphanumeric characters, is generated once at the device 2A and stored in the memory 14 for re-use.

The shared secret PIN may be user generated at the device 2A e.g. the user may input the characters of the shared secret PIN via the input device 18. Alternatively, the device 2A may itself generate the shared secret PIN and display it to the user for sharing.

When a new device attempts to join the network 10, the device 2A automatically, without user intervention, accesses the stored shared secret PIN 15 and uses it in the required pairing process. The user of the device 2A is not therefore disturbed or interrupted. Thus use of a secret PIN that is shared and its storage in the device 2A obviates the need for the user of the

device 2A to re-enter data each time a new device attempts to join the network.

Fig. 3A illustrates a decision process that, in one embodiment, occurs in the device 2A. The device 2A has a plurality of different operational modes. There is at least one mode of operation in which it is undesirable to have interruptions to the user. This mode is typically one in which real time input is required from the user such as an interactive gaming mode. In the interactive gaming mode the network 10 is a gaming network and each of the devices 2 in the network are used to play an interactive game. Any interruption to the user of the device 2A during game play will detract from his enjoyment.

In this example, the memory 14 stores one or more shared secret PINs each of which is associated with an operational mode that should not be interrupted. One of the PINs is, for example, associated with a gaming mode and is used for automatic pairing while the device is in that mode.

Referring to Fig. 3A, at step 30 an initiation signal is received at the low power radio transceiver 12. The initiation signal indicates that the pairing process should occur. Referring to Fig 4, it may, for example, be the message LMP_in_rand or the message LMP_accepted.

At step 32, it is determined whether or not the device is in an interactive gaming mode or similar mode during which the user does not wish to be interrupted. If the device is not in a gaming mode the process branches to step 33, but if the device is in a gaming mode the process branches to step 34.

At step 33, a data screen or dialog is presented on the display 17 requesting the user input of data. The data entered is used as the PIN in the pairing process at step 35.

At step 34, the shared secret PIN 15 associated with the current mode of the device is read from the memory 14 for use in the pairing process at step 36.

It will therefore be appreciated that when a user is playing a game on a device that is Master of the network, he is not required to agree and enter a PIN each time a new user joins the network. A shared network PIN is defined to avoid repeated distribution of new PINs. The shared PIN is stored to prevent repeated user entry. The pairing process is initiated automatically without user intervention, thereby avoiding interruptions to the user.

The shared network PIN may be defined separately from and before the process of joining a new user to the network by pairing, for example, via a menu feature. Alternatively, the shared network PIN may be defined on creating the interactive network as a consequence of the first pairing process for that network. The PIN used for that first pairing process is then stored for re-use during the pairing processes when additional users join that network. Thus when additional users join the network the contemporaneous input of a PIN is not required at the master.

The device may allow a user to select which operational modes should not be interrupted.

Fig. 3B illustrates a decision process that, in one embodiment, occurs in the device 2A. The device 2A provides one or more different services.

In this example, the memory 14 stores one or more shared secret PINs each of which is associated with a service provided by the device. One of the PINs may, for example, be associated with a gaming service and is used for automatic pairing prior to the provision of that service. One of the PINs may, for example, be associated with a mobile cellular telecommunications service and is used for automatic pairing prior to the provision of that service.

Referring to Fig. 3B, at step 30 an initiation signal is received at the low power radio transceiver 12. The initiation signal is the start of a request for a required service and indicates that the pairing process should occur. Referring to Fig 4,

it may, for example, be the message LMP_in_rand or the message LMP_accepted.

At step 32', it is determined whether or not the initiation signal is initiating a service that has an associated shared secret PIN. If there is no stored PIN associated with the required service or the required service cannot be identified then the process branches to step 33. If there is a stored PIN associated with the required service then the process branches to step 34.

At step 33, a data screen or dialog is presented on the display 17 requesting the user input of data. The data entered is used as the PIN in the pairing process at step 35.

At step 34, the shared secret PIN 15 associated with the required service is read from the memory 14 for use in the pairing process at step 36.

It will therefore be appreciated that whenever a new user requests a service from the Master, the user of the Master is not necessarily required to agree and enter a PIN. A shared network PIN is defined to avoid repeated distribution of new PINs. The shared PIN is stored to prevent repeated user entry. The pairing process is initiated automatically without user intervention, thereby avoiding interruptions to the user.

The shared network PIN may be defined separately from and before the process of joining a new user to the network by pairing, for example, via a menu feature. Alternatively, the shared network PIN may be defined on as a consequence of a first pairing process for a particular service. The PIN used for that first pairing process is then stored for re-use during the pairing processes when additional users join the network for that service. Thus when additional users join the network the contemporaneous input of a PIN is not required at the master.

The device may allow a user to select which service should have an associated PIN and to define the characters of the PIN.

In Fig. 4, an Initiator device initiates the pairing process and a Responder device responds. Typically the Initiator device will be a candidate Slave device seeking to join the network as a Slave and the Responder device will be the Master of the network. However, the roles may be reversed.

The stored shared secret PIN 15 is made available to those persons who the user of the Master wishes to be able to join the network 10. Typically this will be by verbal communication between the user of the Master and the other persons. In other embodiments it may be possible for the Master to communicate the stored shared secret PIN to other devices. However, such communication should not be via the network 10 if this would compromise the secrecy of the shared secret PIN 15. It may, if the devices are also mobile telephones, be via a data messaging service provided by a mobile telephone network, for example, SMS messaging.

The Initiator generates a random number RAND, at stage 21. At stage 22, the Initiator sends the random number RAND to the Responder in the signal LMP_in_rand. The Responder replies with LMP_accepted.

At stage 23, the user of the Master device is not required to input data. The device automatically accesses the shared secret PIN 15 that is stored in the memory 14. The user of the candidate Slave device manually inputs the shared secret PIN.

The candidate Slave device may save the shared secret PIN for future use when it is master of the piconet.

At stage 24, there is symmetric creation of an initialization key Kinit at both the Initiator and the Responder. The algorithm for creating Kinit takes as its inputs the random number RAND, the shared secret PIN, and the Bluetooth Device address (BD_ADDR) of the Responder device. The BD_ADDR is an identifier of the Responder Device that is permanently stored in the Responder device

and is previously transferred to the Initiator device e.g. during the Inquiry procedure. The initialisation key Kinit is used to enable authentication.

At stage 25, there is a handshake between the Responder and the Initiator to determine whether a combination link key or a unit link key should be used as a common link key.

At stage 26, the common link key is generated and shared between the Initiator and Responder. The common link key is used in authentication between the two devices for all subsequent connections until it is changed.

The Responder and Initiator use the same algorithm to generate the link key.

If a unit link key is to be used, the initialisation key Kinit is used to encrypt the unit link key during communication from one device to the other via the network 1. If for example, the unit link key of the Initiator is to be used, it is XORed with Kinit and the result is sent to the Responder, where it is XORed with Kinit to recover the original unit link key.

If a combination link key is used, an Initiator specific link key is created in the Initiator using its Bluetooth device address (BD_ADDR) and a locally generated random number, and a Responder specific link key is created in the Responder using its Bluetooth device address (BD_ADDR) and a locally generated random number. The Initiator and Responder then exchange their locally generated random numbers. The Initiator then creates the Responder specific link key and the Responder creates the Initiator specific link key. Each of the Responder and Initiator then creates the same combination link key using both the Responder specific link key and the Initiator specific link key.

The initialisation key Kinit is used to encrypt the locally generated random numbers before they are exchanged via the network 10. The random number key is XORed with Kinit at its origin and the result when received at the destination is XORed with Kinit to recover the random number.

Thus the Initialisation key Kinit is used in the generation and sharing of the link key.

At stage 27, mutual authentication based on the common link key occurs. The common link key is used in a challenge response mechanism. A first signed response is calculated in the Responder based on at least a random value and the common link key. The random value is transferred to the Initiator where a second signed response is calculated based on at least the transferred random value and the common link key. The second signed response is transferred to the Responder and compared with the first signed response. If they agree the Initiator is authenticated by the Responder.
The process is mutual because the Responder is then authenticated by the Responder.

Although embodiments of the present invention have been described in the preceding paragraphs with reference to various examples, it should be appreciated that modifications to the examples given can be made without departing from the scope of the invention as claimed. For example, although the above described embodiments relate a Bluetooth network, embodiments of the invention are not limited to Bluetooth networks and devices nor are they limited to a network with a star topology. In Bluetooth, encryption and authentication are separated, so a separate encryption key is generated if required. However, in other systems, the equivalent of the common link key could also be used in addition or in the alternative for encryption. Also the key created directly from the shared secret PIN could be used, in systems less secure than Bluetooth, as an authentication key or an encryption key.

Whilst endeavouring in the foregoing specification to draw attention to those features of the invention believed to be of particular importance it should be understood that the Applicant claims protection in respect of any patentable feature or combination of features hereinbefore referred to and/or shown in the drawings whether or not particular emphasis has been placed thereon.

I/we claim: